BUNDESREPUBLIK DEUTSCHLAND

09/937819

DE 00/189
EJU

Bescheinigung

Die Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung eV in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Vorrichtung und Verfahren für die sichere elektronische Datenübertragung"

am 29. März 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol H 04 L 9/30 der Internationalen Patentklassifikation erhalten.

München, den 28. Februar 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Aktenzeichen: 199 14 225.4

Wallner

Vorrichtung und Verfahren für die sichere elektronische Datenübertragung

Die Erfindung betrifft eine Vorrichtung sowie ein Verfahren für die sichere elektronische Datenübertragung zwischen Endgeräten, die zeitweilig oder permanent mit einem Server verbunden sind.

Das Verfahren und die Vorrichtung sind insbesondere für die elektronische Weitergabe medizinischer Daten sehr gut geeignet.

Medizinische Daten stellen aus der rechtlichen Sicht des Datenschutzes eines der schützenswertesten Güter überhaupt dar. Für die elektronische Weitergabe medizinischer Daten über öffentlich zugängliche Netze, wie beispielsweise das Internet oder ein von außen zugängliches Verbundnetz, sind daher Sicherheitsmaßnahmen vorzusehen, die den bestmöglichen Schutz solcher Daten gewährleisten.

Die grundsätzlich für die Datenübertragung durch öffentliche Netze verfügbaren Sicherheitsmechanismen betreffen vor allem die Nutzung kryptographischer Verfahren zur Verschlüsselung der Daten. Hierbei werden in der Regel kryptographische Standardverfahren mit sicherem Austausch von Schlüsseln entsprechend X.509 eingesetzt. Dabei handelt es sich um symmetrische Verschlüsselungsverfahren, insbesondere für die Verschlüsselung großer Datenmengen, und um asymmetrische Verschlüsselungsverfahren unter Verwendung eines öffentlichen (sog. "public key") und eines

privaten Schlüssels (sog. "private key"), wie das weit verbreitete RSA.

Die vorliegende Erfindung betrifft die Übertragung von Daten von einem Netzteilnehmer (Absender) zu einem anderen (Adressat bzw. Empfänger) über die Zwischenspeicherung auf einer Datenstation bzw. einem Server. Während bei der elektronischen Datenübertragung über das Netz von einem Teilnehmer zu einem bereits bekannten Adressaten ein asymmetrisches Verschlüsselungsverfahren unter Verwendung des öffentlichen Schlüssels des Adressaten zur Verschlüsselung der Daten eine hohe Datensicherheit bietet, kann diese Vorgehensweise bei einem zum Zeitpunkt der Bereitstellung der Daten noch unbekannten Adressaten nicht eingesetzt werden.

Ein solcher Fall ergibt sich beispielsweise im medizinischen Bereich, wie weiter unten im Ausführungsbeispiel näher erläutert wird, wenn ein Arzt einem Patienten eine Überweisung an einen Kollegen ausstellt und die für den Arztkollegen bestimmten medizinischen Daten des Patienten auf elektronischem Wege bereitstellen will. Die Identität des Kollegen, den der Patient schließlich aufsuchen wird, ist zu diesem Zeitpunkt in vielen Fällen noch nicht bekannt.

Die Aufgabe der vorliegenden Erfindung besteht nun darin, eine Vorrichtung und ein Verfahren für die sichere elektronische Datenübertragung über den Server eines Netzwerkes bereitzustellen, bei dem der Adressat der Daten zum Zeitpunkt der Bereitstellung der Daten noch nicht bekannt sein muß.

Die Aufgabe wird mit der Vorrichtung und dem Verfahren nach den Ansprüchen 1 und 12 gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen des Verfahrens und der Vorrichtung sind Gegenstand der Unteransprüche.

Die erfindungsgemäße Vorrichtung, die am Server des Netzwerkes installiert und betrieben werden muß, weist eine Eingangseinheit zum Empfangen von verschlüsselten Daten (des Absenders) sowie eines externen Schlüssels (des Empfängers) auf. Weiterhin ist in der Vorrichtung eine Einheit zum Entschlüsseln der verschlüsselten Daten mit einem internen Schlüssel und zum erneuten Verschlüsseln der Daten mit dem externen Schlüssel vorgesehen. Der interne Schlüssel ist innerhalb der Vorrichtung in irgendeiner technischen Form abgelegt und von außerhalb der Vorrichtung nicht zugänglich. An einer Ausgangseinheit können die mit dem externen Schlüssel verschlüsselten Daten abgegriffen werden.

Es versteht sich von selbst, daß die von der Vorrichtung zu verarbeitenden Daten so verschlüsselt sein müssen, daß sie mit dem internen Schlüssel der Vorrichtung entschlüsselt werden können. In der Vorrichtung werden somit nur für die Vorrichtung lesbare verschlüsselte Daten mit einem externen Schlüssel zur Neuverschlüsselung umgewandelt in neu verschlüsselte Daten, die für den Inhaber des bei einer entsprechenden Datenanforderung mit den Daten an die Vorrichtung übergebenen externen Schlüssels lesbar sind.

Hierbei ist es grundsätzlich möglich, die zu übertragenden Ursprungsdaten, d.h. beispielsweise medizinische Daten, von der Vorrichtung entschlüsseln sowie neu verschlüsseln zu lassen. Bei dem bevorzugten Einsatz der Vorrichtung, wie weiter unten ausgeführt, werden allerdings nicht die Ursprungsdaten selbst, sondern nur deren in verschlüsselter Form übertragener Schlüssel mit der Vorrichtung neu verschlüsselt.

In einer bevorzugten Ausführungsform weist die Vorrichtung zum Entschlüsseln der verschlüsselten Daten sowie zur Neuverschlüsselung der Daten eine Chipkarte als Träger des internen Schlüssels auf. Bei dieser Chipkarte handelt es sich vorzugsweise um eine Chipkarte eines zertifizierten Trust-Centers.

In einer weiteren Ausprägung können Verschlüsselung und Entschlüsselung ganz oder teilweise direkt durch eine aktive Chipkarte ausgeführt werden.

Eine weitere Möglichkeit besteht darin, eine nach dem Informations- und Kommunikationsdienste-Gesetz sowie Signaturgesetz geeignete Schaltung, gegebenenfalls Software-gesteuert als Einheit zur Ver- und Entschlüsselung einzusetzen.

Kern der erfindungsgemäßen Lösung ist eine Umschlüsselung der Daten oder eines den Daten anhängenden Schlüssels, im folgenden als Session-Key bezeichnet, so daß die Daten für einen der berechtigten Kommunikationspartner, den Adressaten, lesbar werden. Dazu wird in der bevorzugten Ausführungsform des Verfahrens ein für die symmetrische Verschlüsselung der Daten verwendeter Session-Key mit dem im Server vorhandenen priva-

ten Schlüssel des Servers entschlüsselt und sofort wieder mit dem öffentlichen Schlüssel des die Daten anfordernden Empfängers bzw. Adressaten verschlüsselt. Dieser Schlüssel ist vorzugsweise - z.B. zusammen mit der Teilnehmer-ID und der ISDN-Nummer - in einem Verzeichnis der beteiligten und berechtigten Netzteilnehmer auf dem Server gespeichert und kann bei Bedarf über die Dienste eines Trust-Centers jederzeit aktualisiert werden.

Ein Entschlüsseln der Ursprungsdaten selbst ist bei diesem Verfahren nicht notwendig. Zum späteren Entschlüsseln der Daten muß nur der - jetzt für den Empfänger lesbare - Session-Key bekannt sein, der bei der Verschlüsselung beispielsweise per Zufall generiert wurde, wie im Ausführungsbeispiel näher erläutert wird.

Auf diese Weise wird vermieden, daß die Daten selbst zu irgendeinem Zeitpunkt auf dem Server in unverschlüsselter Form vorliegen. Im Detail bedeutet dies, daß auf die verschlüsselten Daten während des Umschlüsselungsprozesses überhaupt kein Zugriff erfolgt. Verarbeitet wird lediglich der für Ihre Verschlüsselung verwendete Session-Key, der in einem geschlossenen Prozeß aus einer nur für den Server bzw. die am Server installierte erfindungsgemäße Vorrichtung lesbaren in eine für den Anfordernden lesbare Form "umgeschlüsselt" wird.

Der Einsatz der Vorrichtung soll im nachfolgenden anhand eines Ausführungsbeispiels in Verbindung mit der Figur näher erläutert werden. Dieses Beispiel betrifft einen Anwendungsfall im medizinischen Bereich, der ein

bevorzugtes Anwendungsfeld der vorliegenden Erfindung darstellt.

Hierbei werden in Kombination mit der erfindungsgemäßen Vorrichtung sowie dem erfindungsgemäßen Verfahren weitere, für sich genommen bereits bekannte Sicherheitsmaßnahmen beschrieben und vorgenommen, die insgesamt eine hochsichere Datenweitergabe in dem genannten Anwendungsfall gewährleisten.

Es versteht sich von selbst, daß die nachfolgend angeführten Kombinationen der einzelnen Sicherheitsmaßnahmen unabhängig voneinander sind, so daß auch die Auslassung eines dieser Schritte, oder der Ersatz durch andere bekannte Sicherheitsmaßnahmen, möglich sind.

Das Beispiel betrifft die elektronische Weitergabe medizinischer Daten über öffentliche Netze. Die hierfür eingesetzten Sicherheitsmaßnahmen gewährleisten den bestmöglichen Schutz dieser sensiblen Daten. Ein typischer Vorgang in diesem Bereich beginnt in der Praxis des Arztes eines Patienten. Der Arzt überweist den Patienten an einen Facharzt, der diesem aufgrund des freien Arztwahlrechtes des Patienten zu diesem Zeitpunkt noch nicht bekannt ist. Üblicherweise wurden dem Patienten bisher hierzu in einem verschlossenen Umschlag die für den Facharzt wichtigen medizinischen Daten zusammen mit der Überweisung übergeben, der diese dem von ihm gewählten Facharzt dann weitergegeben hat.

Wollte der Arzt diese Daten dem Kollegen auf elektronischem Wege übermitteln, so mußte er bisher die Identität dieses Kollegen zum Zeitpunkt der Überweisung bereits kennen. Dies ist mit dem im folgenden geschilderten Verfahren unter Einsatz der erfindungsgemäßen Vorrichtung und des erfindungsgemäßen Verfahrens nicht

mehr erforderlich. Das zugrunde liegende System sieht zumindest eine zentrale Datenstation, einen Server, vor, zu dem von Datenstationen der am System beteiligten Stellen, im vorliegenden Fall den externen Rechnern der Ärzte, eine Verbindung hergestellt werden kann. Bezogen auf den oben dargestellten Fall bedeutet dies, daß der überweisende Arzt die für den (noch unbekannten) Kollegen vorgesehenen medizinischen Daten des Patienten auf dem Server ablegt, von dem sich der Kollege diese Daten dann zu einem späteren Zeitpunkt holen kann.

Die Beschreibung der Sicherheitsmechanismen geht dabei zunächst von allgemeinen Sicherheitsaspekten des Systemdesigns aus, beschreibt dann die allgemeine und spezielle Nutzung kryptographischer Verfahren und schließlich die Einbindung und technische Umsetzung der erfindungsgemäßen Vorrichtung.

Jede Form des aktiven Lesens von Daten erfordert ein - gegebenenfalls eingeschränktes - Zugriffsrecht auf die Datenstation, auf der die Daten gespeichert sind. Im vorliegenden Beispiel gestattet das System keinen lesenden Zugriff auf den Server, sondern nur das Absetzen einer Datenanforderung durch die beteiligten Stellen. Bei nachgewiesener Empfangsberechtigung werden die Daten dem Anforderer, im vorliegenden Beispiel also dem die Daten anfordernden Facharzt, über das Netz zugeschickt. Dadurch werden direkte Zugriffe einer externen Stelle auf Datenbestände des Servers weitestgehend unterbunden.

Das beispielhafte Konzept verwendet für die Kommunikation eine Kommunikationsart, die als "remote procedure call" (RPC) bekannt ist. Dabei wird vom externen Rechner eine Aufforderung an den Server gesendet, eine bestimmte Funktion auszuführen und das Ergebnis dieser Funktion als Resultat zurückzugeben. Der Vorteil dieser Kommunikation ist, daß auf dem Server eine problemspezifische Applikation läuft, die nur genau die Operationen ausführt, die in der System-funktion vorgesehen sind. Darüber hinausgehende Funktionen, wie z.B. ein direkter Dateizugriff, sind auf diese Weise absolut sicher ausgeschlossen.

Das Konzept sieht weiterhin vor, daß ein Netzteilnehmer zum Aufbau einer Verbindung zunächst immer eine Aufforderung zum Verbindungsaufbau an den Server schickt. Bei dieser Operation selbst erfolgt noch kein Verbindungsaufbau. Es ist vielmehr vorgesehen, diese Anforderung als sogenannte "D-Kanal-Nachricht" zu realisieren. Dabei handelt es sich um eine spezielle Funktion des ISDN-Netzes, bei der noch vor dem "Annehmen" eines Gespräches - damit auch gebührenfrei - nur die Kennung bzw. Nummer des Anrufers übermittelt wird. Anschließend prüft der Server die Übereinstimmung dieser Nummer mit einer am Server gespeicherten Teilnehmerliste, und nur wenn die übermittelte Nummer des Anrufers zu einem "berechtigten" Netzteilnehmer gehört, initiiert der Server einen Rückruf über eine in einer internen Datenbank gespeicherte Nummer.

Der besondere Sicherheitsaspekt dieser Lösung besteht darin, daß zwar die im D-Kanal übertragene Nummer des Anrufers unter bestimmten Umständen

fälschbar ("maskierbar") ist, die Verbindung durch den Server aber in jedem Fall mit dem tatsächlichen Inhaber dieser Nummer, also einen berechtigten Netzteilnehmer aufgebaut wird. Damit wird im ungünstigsten Falle ein Verbindungsaufbau zu einem Netzteilnehmer angestoßen, der diesen gar nicht angefordert hatte, jedoch zum Kreis der Berechtigten gehört. In einem derartigen Fall kann es zu keiner Datenübertragung kommen, da der Rechner des unaufgefordert zurückgerufenen Teilnehmers keine Datenanforderung bereithält, und damit auch nicht zum Verbindungsaufbau bereit ist.

Das vorliegend beschriebene beispielhafte Konzept basiert darauf, Dokumente im Sinne eines "Mailings" einmalig zu übertragen. Sobald ein Dokument vom Server durch einen berechtigten Adressaten abgefordert und diesem zugestellt wurde, wird es auf dem Server gelöscht (zunächst logisch, dann auch physisch). Dies ist speziell im vorliegenden Anwendungsfall möglich, da die Daten jeweils nur für einen Adressaten vorgesehen sind. Sollen die Daten mehreren Adressaten zugänglich sein, wird diese Maßnahme nicht vorgesehen.

Alle Dokumente werden weiterhin mit einem Verfallsdatum versehen, nach dessen Ablauf sie ebenfalls physisch gelöscht werden. Damit entsteht keine Akkumulation von Daten auf dem Server, womit auch die Zusammenführung von unterschiedlichen Dokumenten, die etwas über einen Patienten oder auch über einen Arzt aussagen könnten, unmöglich gemacht wird. Die Identifikation der Dokumente erfolgt über eine einmalig nur für diesen Kommunikationsvorgang vergebene Vorgangs-ID, die keinen Rückschluß auf den Patienten zuläßt. Diese ID muß dem anfordernden Arzt bekannt sein, und wird ihm

vorzugsweise mit dem zugehörigen Papierdokument durch den Patienten übermittelt.

Zusätzlich zu den oben beschriebenen Sicherheitsmaßnahmen werden alle Daten für die Übertragung und Speicherung verschlüsselt und signiert. Dazu werden kryptographische Standardverfahren mit sicherem Austausch von Schlüsseln, beispielsweise entsprechend X.509, eingesetzt. Dabei handelt es sich um symmetrische Verschlüsselungsverfahren wie Triple DES, "blowfish" oder IDEA für die Verschlüsselung großer Datenmengen und asymmetrische Verschlüsselungsverfahren wie RSA oder elliptische Verschlüsselungsverfahren für die digitale Signatur (Verschlüsselung eines Hash-Wertes) und die Verschlüsselung des symmetrischen Session-Keys.

Zur Sicherung der Authentizität und Integrität der übertragenen Daten wird jedes Dokument vor dem Versand mit dem privaten Schlüssel des Absenders, im vorliegenden Fall des überweisenden Arztes, signiert. Dazu wird ein Hash-Wert ermittelt und dieser mit dem privaten Schlüssel des Absenders asymmetrisch verschlüsselt. Die Signatur des Dokumentes bleibt auch nach dem Entschlüsseln (siehe nachfolgende Schritte) erhalten und steht somit für den forensisch relevanten Nachweis der Echtheit des Dokumentes zur Verfügung. Voraussetzung für den Nachweis der Echtheit ist allerdings, daß das Dokument beim Empfänger in der signierten Form gespeichert wird, gegebenenfalls zusätzlich zur lesbaren Version ohne Signatur. Ein getrenntes Speichern von Dokument und Signatur ist möglich, birgt jedoch die Gefahr, daß durch ungewollte Modifikation des Dokumen-

tes - z.B. beim Öffnen im Textverarbeitungssystem - die Signatur ungültig wird. Die Archivierung des Dokuments obliegt dem Empfänger.

Die Einzeldokumente werden mit einem zufällig generierten Schlüssel (Session-Key) der Länge N (N sollte aus Sicherheitsgründen größer oder gleich 128 sein) symmetrisch verschlüsselt. Der zum Verschlüsseln verwendete Session-Key wird mit dem öffentlichen Schlüssel des Servers, d.h. der am Server installierten erfindungsgemäßen Vorrichtung, verschlüsselt. Die Schlüssellänge sollte aus Sicherheitsgründen mindestens 1024 Bit betragen.

Da das Dokument inklusive Signatur verschlüsselt wird, kann der Server ohne Entschlüsselung der Daten die Echtheit des Dokumentes - auch im Sinne seiner fehlerfreien Übertragung und seiner Existenz an sich (elektronisches "Einschreiben") - nicht überprüfen. Um dies zu ermöglichen, wird das signierte und verschlüsselte Dokument nochmals zusätzlich signiert.

Das wie oben beschrieben vorbereitete Dokument wird als MIME-kompatibles File aufbereitet und in dieser Form mittels eines entsprechenden RPC an den Server übermittelt.

Auf dem Server wird das Dokument aus dem MIME-Format entpackt und die äußere Signatur kontrolliert und dabei entfernt. Damit wird die Unversehrtheit, d.h. die Vollständigkeit und Originalität, des Dokumentes überprüft und kann protokolliert werden. Nach erfolgter Ablage des (verschlüsselten) Dokumentes wird eine vom

Server mit dessen persönlichem Schlüssel signierte Empfangsbestätigung an den Absender zurückgegeben als zweifelsfreier Nachweis der erfolgten Ablage des Dokumentes.

Das weiterzuleitende Dokument wird auf dem Server in der (innen) signierten und dann verschlüsselten Form gespeichert. In dieser verschlüsselten Form ist es von niemandem zu entschlüsseln.

Als Ablage- bzw. Zugriffskriterium zum Verwalten des verschlüsselten Dokuments dient eine unverschlüsselt mitgelieferte Vorgangs-ID, die zu jedem Vorgang gehört. Diese Vorgangs-ID, wird, wie bereits oben dargelegt, dem später durch den Patienten ausgewählten Arzt durch diesen auf direktem Wege übermittelt. Für den Server ist diese ID aus der übersandten Datenanforderung ersichtlich, deren Bestandteil sie ist.

Daten können vom Server durch Mitglieder des jeweiligen Netzes unter Angabe dieser jeweiligen Vorgangs-ID, ihrer ISDN-Nummer und ihrer Arztkennung angefordert werden.

Zur weiteren Erhöhung der Sicherheit können zusätzliche Identifikatoren, z.B zur Kennzeichnung des jeweiligen Patienten, notwendig sein.

Bei der Anforderung der Daten durch den betreffenden Facharzt erfolgt eine Umschlüsselung der Daten durch die erfindungsgemäße Vorrichtung, so daß sie für einen den anfordernden Arzt lesbar werden. Dazu wird der für die symmetrische Verschlüsselung der Daten verwendete Session-Key mit dem im Server vorhandenen privaten Schlüssel des Servers entschlüsselt und sofort

wieder mit dem öffentlichen Schlüssel des anfordernden Empfängers verschlüsselt. Dieser öffentliche Schlüssel ist - zusammen mit der Arzt-ID und der ISDN-Nummer - im Verzeichnis der beteiligten Netzärzte gespeichert und kann über die Dienste eines einbezogenen Trust-Centers jederzeit aktualisiert werden.

Ein Entschlüsseln der medizinischen Daten selbst ist nicht notwendig. Zum späteren Entschlüsseln der Daten muß nur der - jetzt für den Empfänger lesbare - Session-Key bekannt sein, der bei der Verschlüsselung per Zufall generiert wurde.

Auf diese Weise wird vermieden, daß die medizinischen Daten selbst zu irgendeinem Zeitpunkt auf dem Server in unverschlüsselter Form vorliegen. Auf die verschlüsselten Daten erfolgt während des Umschlüsselungsprozesses keinerlei Zugriff. Verarbeitet wird lediglich der für Ihre Verschlüsselung verwendete Session-Key, der in einem geschlossenen Prozeß aus einer nur für den Server lesbaren in eine für den Anfordernden lesbare Form "umgeschlüsselt" wird.

Das für den Versand an den Empfänger verschlüsselte Dokument wird nochmals zur Sicherung der korrekten Übertragung zum Empfänger und einer eventuell gewünschten Protokollierung signiert, und zwar durch den Server mit dessen persönlichem Schlüssel.

Das wie oben beschrieben vorbereitete Dokument wird wiederum als MIME-kompatibles File aufbereitet und in dieser Form als Rückgabewert eines RPC zur Datenanforderung an den Anforderer geschickt.

Beim Empfänger wird das Dokument aus dem MIME-Format entpackt und die äußere Signatur kontrolliert und dabei entfernt. Damit wird wiederum die Unversehrtheit, d.h. Vollständigkeit und Originalität, des Dokumentes überprüft. Eine vom Empfänger mit dessen persönlichem Schlüssel signierte Empfangsbestätigung wird an den Server zurückgegeben als zweifelsfreier Nachweis der erfolgten Übermittlung des Dokumentes.

Mittels des persönlichen Schlüssels des Empfängers kann dieser den verschlüsselten Session-Key entschlüsseln und mit diesem wiederum die Daten selbst. Danach liegen diese lesbar nur noch in der durch den Absender signierten Form vor.

Die Signatur des Ausgangsdokumentes dient der Nachweisbarkeit seiner Originalität. Um diese zu erhalten ist es notwendig, das Dokument in der signierten Form aufzubewahren.

Ein möglicher Angriffspunkt auf die Daten ist der private Schlüssel des Servers. Da alle eingelagerten Daten - genauer gesagt alle Session-Keys der eingelagerten Daten - mit demselben Schlüssel des Servers lesbar sind, lohnt sich ein Angriff auf diesen Schlüssel einerseits besonders, andererseits wird er durch die Menge vorliegender Daten erleichtert.

Um diesem Umstand vorzubeugen, wird bei einer bevorzugten Ausführungsform der vorliegenden Erfindung als zusätzlicher Sicherheitsmechanismus eine Zweiteilung des Session-Keys eingeführt.

Wie weiter oben beschrieben, werden die Ursprungsdaten mit einem N-stelligen (N vorzugsweise größer oder gleich 128) symmetrischen Schlüssel verschlüsselt. Dieser Schlüssel wird üblicherweise für die Übertragung asymmetrisch und nur für den Empfänger lesbar verschlüsselt. Die - auch gewaltsame - Entschlüsselung des Session-Keys reicht damit aus, um die Daten selbst entschlüsseln zu können.

Um dies zu verhindern, wird folgende Modifikation eingeführt. Bei dieser Modifikation wird der Session-Key vor seiner asymmetrischen Verschlüsselung zweigeteilt. Beispielsweise werden M ($0 < M < N$) der N Bits des Session-Keys als sogenannter "Vorgangsschlüssel" herausgelöst. Nur die verbleibenden (N-M) Bits des Session-Keys werden asymmetrisch verschlüsselt und mit den Daten übertragen.

Die Umschlüsselung der Daten mit reduziertem Session-Key kann in genau derselben Weise erfolgen, wie oben in Zusammenhang mit einem vollständigen Session-Key beschrieben. Da die Daten selbst auch dort nie entschlüsselt werden müssen, ist der vollständige Session-Key nicht notwendig. Es wird lediglich der rudimentäre Session-Key durch den Server entschlüsselt und für den Anforderer wieder verschlüsselt.

Die Entschlüsselung beim Empfänger unterscheidet sich von der oben beschriebenen Vorgehensweise dahingehend, daß nach der Entschlüsselung des Session-Keys mittels privatem Schlüssel des Empfängers dieser Session-Key um die beim Absender separierten M Bits des Vorgangsschlüssels erweitert werden muß. Danach kann die Entschlüsselung wie oben dargestellt erfolgen.

Der beim Absender der Daten erzeugte Vorgangsschlüssel, d.h. die separierten M Bits, wird an die ebenfalls dort erzeugte Vorgangs-ID angefügt. Die Kombination von Vorgangs-ID und Vorgangsschlüssel ergibt die sogenannte Vorgangskennung, die auf dem den Vorgang begleitenden Papierdokument (Überweisungschein, Einweisungsschein, Rezept, ...) aufgedruckt und beim Empfänger erfaßt wird. Der in der Vorgangskennung enthaltene Vorgangsschlüssel wird niemals zum Server übertragen, so daß dort nie alle Informationen zusammenkommen, die ausreichen würden, um ein Dokument tatsächlich zu entschlüsseln.

Ein Beispiel für eine erfindungsgemäße Vorrichtung, wie sie für die Durchführung des obigen Anwendungsbeispiels eingesetzt wird, ist in Figur 1 dargestellt.

Die Vorrichtung ist vorzugsweise in Form eines Einsteckmoduls 1 (Umschlüsselungsmodul) zum modularen Einbau in den Server ausgebildet. Das Modul 1 beinhaltet im vorliegenden Beispiel eine Chipkarte 2, die die Entschlüsselung des verschlüsselten Session-Keys 10a mit Hilfe des in der Chipkarte 2 gespeicherten privaten Schlüssels des Servers und die erneute Verschlüsselung des Session-Keys mit dem öffentlichen Schlüssel des Adressaten bzw. Anfordernden der Daten vornimmt. Der private Schlüssel des Servers ist dabei von außerhalb der Chipkarte bzw. des Moduls nicht zugänglich. Der öffentliche Schlüssel des Anfordernden wird der Vorrichtung 1, ebenso wie der umzuschlüsselnde Session-Key 10a über eine dafür vorgesehene Schnitt-

stelle zugeführt. Über eine weitere Schnittstelle wird der neu verschlüsselte Session-Key 10b ausgegeben.

Der Prozessor des Servers selbst übernimmt hierbei die Aufgabe, den Session-Key 10a von dem verschlüsselten Datenblock 11 abzutrennen, der Vorrichtung 1 zuzuführen und den von der Vorrichtung gelieferten, neu verschlüsselten bzw. umgeschlüsselten Session-Key 10b wieder an den Datenblock 11 anzufügen, wie in der Figur schematisch dargestellt ist.

Es ist allerdings auch möglich, diese Trennung und erneute Zusammenführung direkt in der Vorrichtung 1 vorzunehmen. Hierbei müßte der Vorrichtung der gesamte Datenblock 11 mit dem Session-Key 10a zugeführt werden.

Der persönliche Schlüssel des Servers ist zweifelsohne ein problematischer Punkt im Hinblick auf gezielte unberechtigte Zugriffsversuche auf die Daten.

Üblicherweise dürfen bzw. sollten Schlüssel nicht auf dem Rechner gespeichert werden, auf dem die verschlüsselten Daten gespeichert bzw. bearbeitet werden. Dies ist jedoch bei automatischer Arbeit des Servers, wie im vorliegenden Fall, unumgänglich. Aus diesem Grunde ist im vorliegenden Ausführungsbeispiel vorgesehen, die Vorrichtung als gekapselte und plombierte Einheit auszugestalten, die in der Lage ist, die vollständige Prozedur der Datenumschlüsselung intern zu handhaben, ohne daß der entschlüsselte (auch rudimentäre) Session-Key oder auch nur Spuren seiner Entschlüsselung die autonome Einheit verlassen.

Heutzutage sind bereits Schlüsselkarten am Markt verfügbar, die in der Lage sind, die asymmetrische Verschlüsselung eines 128 Bit Session-Keys nach einem

1024 Bit RSA-Verfahren vollständig auf dem Chip der Karte auszuführen. Demnächst werden solche Karten auch für 2048 Bit Schlüssel zur Verfügung stehen. Insbesondere besteht die Möglichkeit, das Schlüsselpaar (öffentlicher Schlüssel - privater Schlüssel) direkt auf der Karte oder in einem gesetzeskonformen, zertifizierten Trust-Center generieren zu lassen, ohne daß der private Schlüssel der Karte diese jemals verläßt. Eine solche Schlüsselkarte kann in der erfindungsgemäßen Vorrichtung als Chipkarte 2 eingesetzt werden. Hierbei wird dieser Karte 2 in einem ersten Schritt zunächst der verschlüsselte Session-Key 10a zugeführt. Dieser wird mit Hilfe des privaten Schlüssels des Karte, weiter oben als der private Schlüssel des Servers bezeichnet, entschlüsselt. Der entschlüsselte Session-Key wird von der Karte 2 ausgegeben, ohne die Vorrichtung 1 jedoch zu verlassen. Er wird vielmehr in einem zweiten Schritt der Karte 2 erneut, diesmal zusammen mit dem öffentlichen Schlüssel des Adressaten eingegeben. Die Karte 2 liefert in diesem zweiten Schritt den neu verschlüsselten Session-Key 10b zurück. Dies ist schematisch durch die Pfeile innerhalb der Vorrichtung 1 in der Figur angedeutet. Die hierfür zusätzlich erforderliche Schaltung, Puffer-Einheit 4, dient u.a. zur zeitlichen Koordination dieser Vorgänge. Diese Puffer-Einheit 4 kann beispielsweise durch einen geeignet programmierten Mikroprozessor oder mittels einer Logikschaltung realisiert werden.

Um zu verhindern, daß aus Modulationen auf der Stromversorgung der Vorrichtung Rückschlüsse auf die internen Abläufe möglich sind, ist in der vorliegenden Ausführungsform der Vorrichtung eine Konstant-

stromschaltung 3 vorgesehen, die garantiert, daß die Vorrichtung im Rahmen eines definierten Intervalls der Versorgungsspannung eine konstante und modulationsfreie Stromaufnahme vorweist. Bei Unter- oder Überschreiten bestimmter Grenzen der Betriebsspannung oder anderer Betriebsparameter, wie z.B. der Temperatur, schaltet sich die Vorrichtung mit einer Fehlermitteilung ab.

Da auch aus dem Zeitverhalten der Vorrichtung Rückschlüsse auf die internen Vorgänge gezogen werden könnten, können alle Eingangsdaten zunächst in der Puffer-Einheit 4 oder einer speziell dafür vorgesehenen Einheit gepuffert, und nach einer ständig gleichen Zeit die Ergebnisse ausgegeben werden, unabhängig davon, weiche Zeit die internen Abläufe in Anspruch genommen haben.

Ein "Abhören" der elektromagnetischen Vorgänge in der Vorrichtung wird im vorliegenden Ausführungsbeispiel durch eine elektromagnetische Abschirmung 5 der Vorrichtung verhindert.

Als Schnittstelle der Vorrichtung ist einerseits eine Schnittstelle für die Eingabe des asymmetrisch verschlüsselten Session-Keys 10a (bzw. des Rudimentes dieses Schlüssels) und des öffentlichen Schlüssels des anfordernden Empfängers vorgesehen. Andererseits muß eine Schnittstelle für die Ausgabe des asymmetrisch verschlüsselten Session-Keys 10b (bzw. dessen Rudiment) vorhanden sein. Beide Schnittstellen können bei geeigneter Ausführung physikalisch identisch sein.

Weiterhin können für die Erzeugung bzw. Überprüfung von Signaturen Schnittstellen für die

Eingabe des Hash-Wertes des zu signierenden Dokumentes und für die Ausgabe des symmetrisch verschlüsselten Hash-Wertes, d.h. der Signatur vorgesehen sein.

Obwohl die vorangehend beschriebenen Maßnahmen in Zusammenhang mit dem zugrunde liegenden Beispielfall dargestellt wurden, lassen sich dieses Konzept und die erfindungsgemäße Vorrichtung selbstverständlich auch auf andere Bereiche anwenden, bei denen eine sichere Datenübertragung zwischen zwei Datenstationen über eine Zwischenlagerung auf einem Server erforderlich ist.

Weiterhin ist die Erfindung nicht auf die Weiterleitung der Daten nur über eine Zwischenstation bzw. einen Server beschränkt. So können die Daten auch über mehrere Server geleitet werden, wobei der Abruf der Daten durch einen weiteren Server jeweils wie der Abruf durch einen Adressaten ausgeführt wird. Auf dem weiteren Server werden dann die Daten in gleicher Form wie auf dem ersten Server behandelt, d.h. auch dieser weitere Server muß die erfindungsgemäße Vorrichtung aufweisen.

Patentansprüche

1. Vorrichtung für die sichere Übertragung bzw. Weiterleitung von verschlüsselten Daten über eine Datenstation eines Netzwerkes, mit
- einer Eingangseinheit zum Empfangen der verschlüsselten Daten (10a) sowie eines externen Schlüssels,
- einer Einheit (2) zum Entschlüsseln der verschlüsselten Daten mit einem internen Schlüssel und zum erneuten Verschlüsseln der Daten mit dem externen Schlüssel, wobei der interne Schlüssel von außerhalb der Vorrichtung nicht zugänglich ist; und
- einer Ausgangseinheit zum Ausgeben der mit dem externen Schlüssel verschlüsselten Daten (10b).

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß der interne Schlüssel innerhalb der Einheit (2) zum Entschlüsseln und Verschlüsseln auf einem geeigneten Datenträger gespeichert ist.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln eine Chipkarte als Träger des internen Schlüssels umfaßt.

4. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln eine aktive Chipkarte mit integriertem Prozessor umfaßt, die die Ent- und Verschlüsselung der Daten ganz oder teilweise übernimmt.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß sie eine Puffer- und Logik-Einheit (4) zur zeitlichen Steuerung des Datenflusses in der Vorrichtung aufweist, die der Einheit (2) zum Entschlüsseln und Verschlüsseln zunächst die verschlüsselten Daten (10a) zur Entschlüsselung zuführt und entschlüsselt zurückerhält, und die anschließend der Einheit (2) zum Entschlüsseln und Verschlüsseln die entschlüsselten Daten zur Verschlüsselung mit dem externen Schlüssel zuführt und als verschlüsselte Daten (10b) zurückerhält.

6. Vorrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Eingangseinheit und die Ausgangseinheit Standardschnittstellen für die Ein- und Ausgabe der Daten aufweisen.

7. Vorrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln asymmetrische Verschlüsselungsverfahren einsetzt.

8. Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß sie mit einer vollständigen mechanischen und elektromagnetischen Kapselung (5) und mit einer Möglichkeit zur Versiegelung versehen ist.

9. Vorrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß eine Puffer-Einheit vorgesehen ist, die alle Datenströme innerhalb der Vorrichtung zum Ausgleich von eventuell vom internen Schlüssel abhängigen Verarbeitungszeiten puffert, so

daß die Ausgabe der Daten der Vorrichtung nach einer prozeßunabhängigen Zeitspanne erfolgt.

10. Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß eine Einheit (3) zum Puffern der Stromaufnahme der Vorrichtung vorgesehen ist, so daß die Stromaufnahme der Vorrichtung unabhängig von der vom internen Schlüssel abhängigen Stromaufnahme der Einheit (2) zum Entschlüsseln und Verschlüsseln oder weiterer interner Schaltkreise ist.

11. Vorrichtung nach einem der Ansprüche 1 bis 10, die weiterhin eine Einheit zum Empfangen eines ersten Datenblockes, der die verschlüsselten Daten (10a) neben weiteren Daten (11) beinhaltet, und zum Abtrennen der verschlüsselten Daten (10a) von den weiteren Daten (11) sowie eine Einheit zum Zusammenführen der weiteren Daten (11) mit den erneut verschlüsselten Daten (10b) zu einem zweiten Datenblock und zur Ausgabe des zweiten Datenblockes aufweist, wobei die verschlüsselten Daten einen Schlüssel darstellen, mit dem die weiteren Daten (11) verschlüsselt sind.

12. Verfahren für die sichere Übertragung von Daten von einer ersten Datenstation über eine zweite Datenstation zu einer dritten Datenstation unter Einsatz der Vorrichtung gemäß einem der vorangehenden Ansprüche, mit folgenden Schritten:

- Verschlüsseln der Daten in der ersten Datenstation mit einem ersten Schlüssel;
- Verschlüsseln zumindest eines Teils des ersten Schlüssels in der ersten Datenstation mit einem öffentlichen Schlüssel der zweiten Datenstation;

- Übermitteln der verschlüsselten Daten (11) zusammen mit dem verschlüsselten Teil des ersten Schlüssels (10a) an die zweite Datenstation;
- Speichern der verschlüsselten Daten (11) und des verschlüsselten Teils des ersten Schlüssels (10a) in der zweiten Datenstation;
- Anfordern der Daten durch die dritte Datenstation;
- Entschlüsseln des verschlüsselten Teils des ersten Schlüssels in der zweiten Datenstation mit einem zum öffentlichen Schlüssel passenden privaten Schlüssel der zweiten Datenstation und erneutes Verschlüsseln des vorher entschlüsselten Teils des ersten Schlüssels mit einem öffentlichen Schlüssel der dritten Datenstation; und
- Übermitteln der verschlüsselten Daten (11) zusammen mit dem erneut verschlüsselten Teil des ersten Schlüssels (10b) an die dritte Datenstation.

13. Verfahren nach Anspruch 12, wobei der erste Schlüssel vollständig verschlüsselt und übermittelt wird.

14. Verfahren nach Anspruch 12, wobei nur ein Teil des ersten Schlüssels verschlüsselt und an die zweite Datenstation übermittelt wird.

15. Verfahren nach einem der Ansprüche 12 bis 14, wobei der verschlüsselte Teil des ersten Schlüssels in der dritten Datenstation mit dem privaten Schlüssel der dritten Datenstation entschlüsselt wird, und anschließend die Daten (11) mit dem ersten Schlüssel entschlüsselt werden.

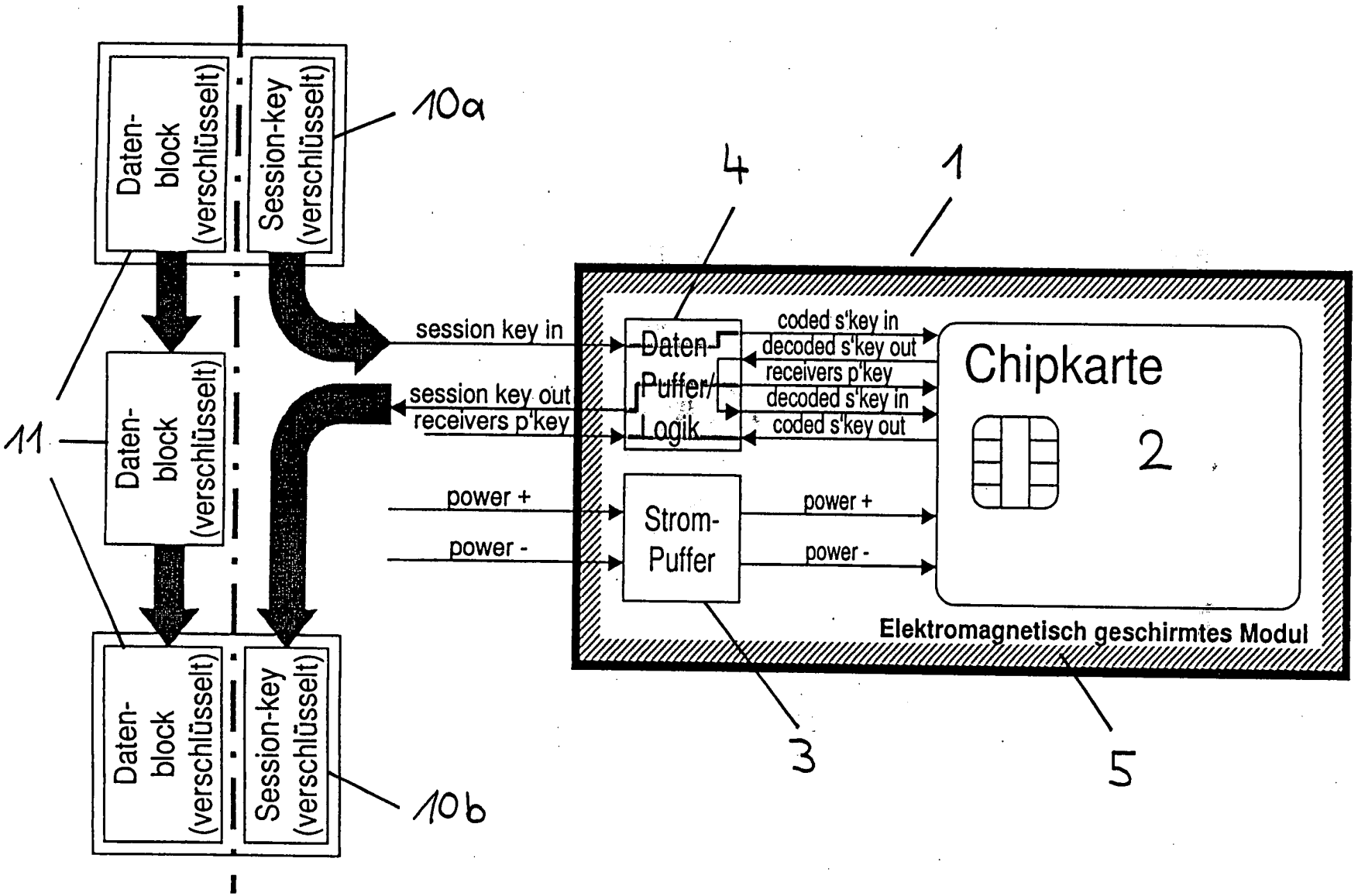
16. Verfahren nach einem der Ansprüche 12 bis 15, wobei der öffentliche Schlüssel der dritten Datenstation aus einer internen Datenbank der zweiten Datenstation entnommen oder durch Rückfrage bei einem Trust-Center ermittelt wird.

Zusammenfassung

Die vorliegende Erfindung betrifft eine Vorrichtung und ein Verfahren zur sicheren elektronischen Datenübertragung über den Server eines Netzwerkes, bei dem der Adressat der Daten zum Zeitpunkt der Bereitstellung der Daten noch nicht bekannt sein muß.

Die Vorrichtung, die am Server des Netzwerkes installiert werden muß, weist eine Eingangseinheit zum Empfangen von verschlüsselten Daten sowie eines externen Schlüssels auf. Weiterhin ist in der Vorrichtung eine Einheit zum Entschlüsseln der verschlüsselten Daten mit einem internen Schlüssel und zum erneuten Verschlüsseln der Daten mit dem externen Schlüssel vorgesehen. Der interne Schlüssel ist von außerhalb der Vorrichtung nicht zugänglich. An einer Ausgangseinheit können die mit dem externen Schlüssel verschlüsselten Daten abgegriffen werden.

Die Daten sind damit für den Inhaber des bei einer entsprechenden Datenanforderung mit den Daten an die Vorrichtung übergebenen externen Schlüssels und damit auch alleinigen Inhaber des zugehörigen internen Schlüssels lesbar.


Daten-block (verschlüsselt)
Session-key (verschlüsselt)
10a
11
Daten-block (verschlüsselt)
Daten-block (verschlüsselt)
Session-key (verschlüsselt)
10b
session key in
session key out
receivers p'key
power +
power -
4
1
Daten-Puffer/ Logik
Strom-Puffer
coded s'key in
decoded s'key out
receivers p'key
decoded s'key in
coded s'key out
power +
power -
Chipkarte
2
Elektromagnetisch geschirmtes Modul
3
5